Google/Apple's contact-tracing apps susceptible to digital attacks

21 July 2022, by Tatyana Woodall

Credit: Pixabay/CC0 Public Domain

Since the beginning of the COVID-19 pandemic, scientists and health authorities have relied on contact-tracing technologies to help manage the spread of the virus. Yet there's a major flaw in a framework that many of these mobile apps utilize—one that attackers could exploit to ramp up false positive notifications.

Apps powered by the Google/Apple Exposure Notification framework (GAEN) are widely available in many countries and operate more efficiently in your phone's background. But researchers from The Ohio State University said they found that these apps are susceptible to geographically based replay attacks, which is when a third party captures a user's broadcasted contact-tracing phone data from one area and exploits it by repeatedly transmitting it in another far-away location.

Replay attacks can be used to exploit electronic weaknesses to gain access to digital networks, cause harmful effects to mobile devices, or poison data sets with false information. Considering how much society relies on honest health data, bad information can be especially harmful in terms of tracking COVID-19, said study co-author Anish Arora, professor and chairperson of computer science and engineering at Ohio State.

"Hackers or nation-state actors could potentially take advantage of an honest user and replay their contact-tracing data anywhere in the world," Arora said.

For example, if someone in Columbus with COVID-19 were to have their contact-tracing beacon data captured by a third party, their information could be transmitted to one or multiple other cities thousands of miles away, and re-broadcasted to others nearby. If this person were to be diagnosed positive for COVID-19, someone who in reality hasn't had any contact with an infected person could be alerted that they have.

That means attackers could essentially create digital superspreaders, starting a process that shares clusters of false exposure beacons in different areas, said Arora.

"Because the framework operates as a wireless protocol, anybody can inject some kind of fake exposure, and those false encounters could disrupt the public's trust for the system," he said.

Although an increase in false-positive notifications would undermine the public good behind contact-tracing apps, co-author Zhiqiang Lin, professor of computer science and engineering at Ohio State, said it could also have cascading economic and social consequences, like causing people to miss work or cancel daily personal activities and long-planned vacations. This potential rises when tests are scarce or in economically disadvantaged countries that don't have access to vaccines, added Lin, who has studied cybersecurity vulnerabilities in digital software for over a decade.

Yet researchers were able to come up with a patch

for this fatal flaw. "The most difficult part was coming up with a fix that was practical and wouldn't inhibit users from using the app," Lin said.

The team came up with a prototype based on Google and Apple's original framework, which they called GAEN+, pronounced "Gain Plus." After implementing it on an Android device (The prototype is also easily portable to Apple devices), they ran the prototype through a series of experiments to test its defenses against malicious replay attacks. They concluded that compared to Google and Apple's framework, GAEN+ was able to effectively prevent false positives while still preserving user privacy.

The team presented their solution on July 12 at the annual meeting of Privacy Enhancing Technologies Symposium (PETS) conference held this year in Sydney, Australia.

Lin said while the team may not be the first to find Google and Apple's flaw, they are currently the first team to prove to the larger digital community how it could be taken advantage of in a "low-cost, distributed manner."

"They may have just thought this couldn't be of severe consequence," he said. But overall, Lin describes their modification to the contact-tracing protocol as "very minimal" for such a strong defense against potential attacks.

"Our enhancement is privacy-preserving," Arora said. Instead of relying on precise GPS data like other proposed fixes, GAEN+ uses coarse location data from Wi-Fi access points and cell phone towers in a clever way that maintains anonymity, he said.

The team did receive thanks from Google for finding and fixing the weakness. To ensure GAEN+ is available to the public, the team has put the source code for the fix on GitHub, a platform that hosts code online.

"When future developers design similar protocols, we're making sure they have the opportunity to consider our recommendations," Arora said. "Both companies made a product that can do a lot of good in the world. We just want to make GAEN much harder to exploit."

Other co-authors were Christopher Ellis and Haohuang Wen, both graduate students in computer science and engineering at Ohio State.

More information: Replay (Far) Away: Exploiting and Fixing Google/Apple Exposure Notification Contact Tracing, *Proceedings on Privacy Enhancing Technologies* (2022).

Provided by The Ohio State University